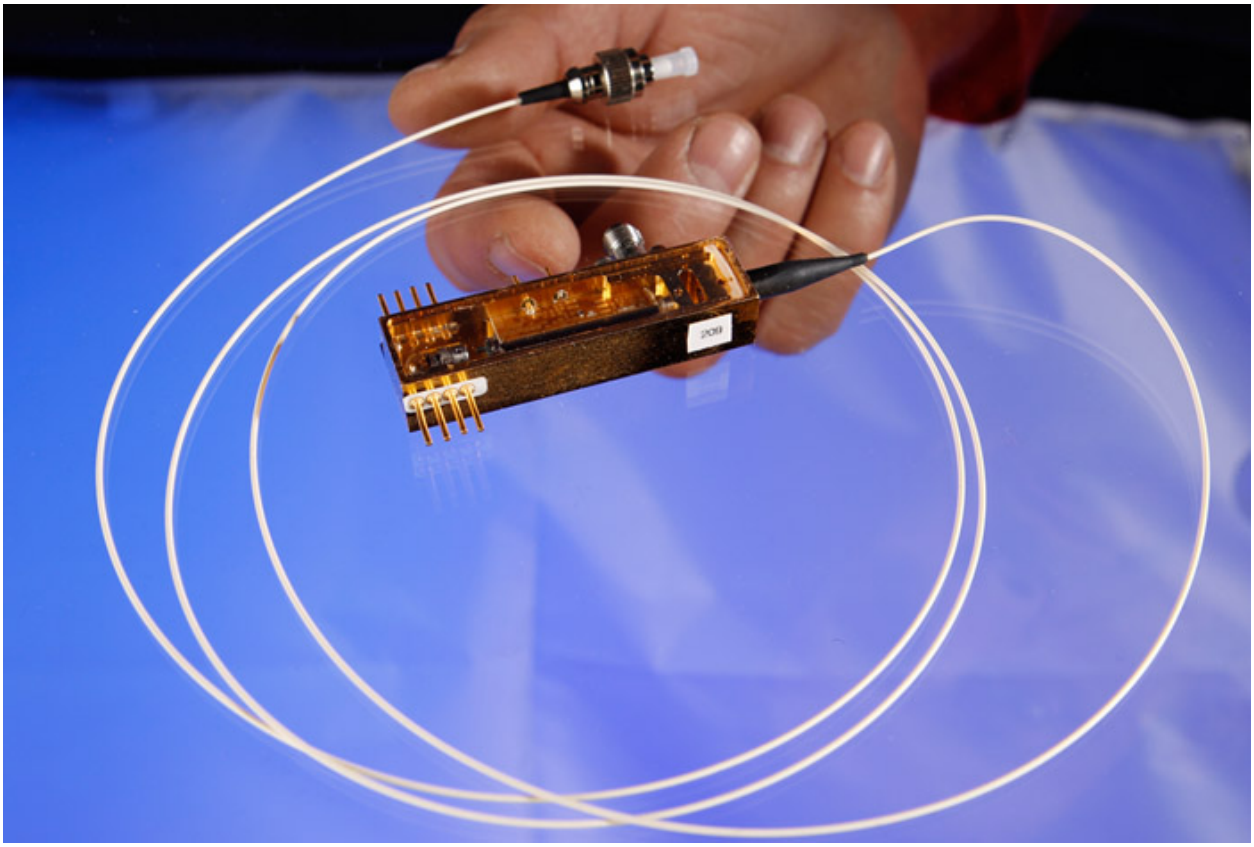
Protecting your personal information

October 1, 2014



Every time you complete an online transaction like purchasing an item over the internet or requesting a bank transfer, you have to trust that your personal data will be kept out of the wrong hands. Banks, credit card companies, retailers and similar entities use sophisticated encryption methods to ensure the information's safety, but as cyber security breaches at large corporations like Target and Home Depot have shown, the current encryption technology is not as safe as was once assumed.

Fortunately, the science of encoding information—cryptography—is beginning a technological revolution that takes advantage of quantum physics and promises encryption that neither today's nor tomorrow's computers can outwit.

Los Alamos National Laboratory's Quantum Communications team, part of the Applied Modern Physics group, has researched and developed quantum cryptography for the past 20 years and is in the process of moving the technology's vast potential for consumer protection into the marketplace.

“Quantum cryptography is very different from current encryption systems,” Quantum Communications team member Raymond Newell explained, “because it takes advantage of the fundamentally unpredictable behavior of individual subatomic particles of light (photons). The very process of trying to eavesdrop on quantum-protected data changes the outcome, which provides a robust layer of defense.”

Thanks to the Quantum Communications team’s efforts, Los Alamos recently signed a technology licensing agreement with Whitewood Encryption Systems, Inc. of Boston, Mass.—the Laboratory’s largest technology transfer contract to date.

“The team owes much of its encryption innovation to physicists Jane E. (Beth) Nordholt and Richard Hughes, who founded and led our efforts for two decades until their retirement this summer,” said Newell. “Both of them still keep track of the ongoing work and, of course, are still connected by way of the existing patents.”

Photons over Los Alamos

The Quantum Communications team already has won important science prizes and set world records. One of the team’s most significant breakthroughs sent single photons flying over Los Alamos in a technically challenging yet perfectly harmless test.

In the team’s so-called “free space” experiment, encryption-carrying photons were transmitted through open air from a source at the Los Alamos Neutron Science Center (LANSCE) to a telescope mounted to a camping trailer parked at the Los Alamos ski hill. The operation was no small feat since the telescope had to differentiate between the incoming experimental photons and the enormous background of daytime light in the natural and human-made environment. Doing the experiment at night only would have helped marginally since the quantity of background photons from moonlight or the lights of Los Alamos still was much larger than the Quantum Communications team’s photon-riding encryption signal.

But the background photons were just part of the problem. Atmospheric distortions caused data losses and posed another set of challenges.

The team was able to successfully address both issues by using interference filters that transmitted only photons of a specific wavelength, by installing a spatial filter at the trailer telescope that only allowed photons arriving from the precise location at LANSCE to pass through, while excluding photons heading toward the telescope from the rest of the world and space—and by relying on a clever trick.

The clever trick was to send a bright laser pulse from LANSCE to the trailer just before a single photon was sent, creating a known delay between the bright pulse and the photon. The delay functioned as an additional “filter” by having the trailer’s telescope accept only photons that entered the system approximately one nanosecond (one billionth of a second) after the bright pulse.

“The multiple-filter approach worked so well,” Newell noted, “that single encryption photons could be distinguished even in broad daylight.”

Team member Glen Peterson was struck by the experiment’s obvious success while operating the system one morning. “The orchestration of physics taking place in front of me was astonishing,” he said. “I knew at that moment we had accomplished something marvelous.”

Today, even though the Los Alamos technology is highly complex in design, it is compact enough that it lends itself to being made into a unit comparable to a computer

thumb drive or compact data-card reader. If everything moves forward as hoped, units could be manufactured at extremely low cost, putting them within easy retail range of mainstream electronics consumers.

For further information, you also might enjoy this issue's personal message by Duncan McBranch, the Laboratory's Chief Technology Officer.